

أرضيات  
2018/5/17  
المادة: منطق

الموضوع: خواصه 8 نظري

دالة أولي: هي الدالة التي تقارن كل عدد طبيعي  $n$  بعدد  $\phi(n)$

$$n \rightarrow \phi(n) = |\mathbb{Z}_n^\times| = \phi(n)$$

$$\mathbb{Z}_n^\times = \{a \in \mathbb{Z}_n : d(a, n) = 1\} \quad \text{حيث } \mathbb{Z}_n = \{0, 1, 2, 3, \dots, n-1\}$$

$$\mathbb{Z}_n^\times = \{1, 3, 5, 7, 9, 11, 13, 15\}$$

مبرهنة أولي: إذا كان  $a$  عدداً صحيحاً و  $n$  عدداً طبيعياً بحيث أوليات  $n$  لا يقسمها  $a$ ،  $d(a, n) = 1$  عندئذٍ

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

الإثبات: (نستخدم نظرية المجموعات)

$$\mathbb{Z}_n^\times = \{\bar{a} \in \mathbb{Z}_n : d(a, n) = 1\}$$

$$\bar{a} \in \mathbb{Z}_n^\times \Leftrightarrow d(a, n) = 1$$

ومن ثم فإن مجموعة  $\mathbb{Z}_n^\times$  تشكل زمرة تحت الضرب.

$$(\bar{a})^{\phi(n)} = \bar{1}$$

ومن ثم

$$(\bar{a})^{\phi(n)} = \bar{1} \Rightarrow a^{\phi(n)} \equiv 1 \pmod{n}$$

$$\Leftrightarrow a^{\phi(n)} \equiv 1 \pmod{n}$$

وهو المطلوب.

$$x \equiv y \pmod{n} \Leftrightarrow x - y = kn$$

نتيجة: إذا كانت  $a$  عدداً صحيحاً و  $p$  عدداً أولياً و  $p$  لا يقسم  $a$ ، فإن

$$a^{p-1} \equiv 1 \pmod{p}$$

فإن

$$p \nmid a$$

$$p \nmid a \Rightarrow d(p, a) = 1$$

$$\phi(p) = p-1$$

فإن

ومن ثم فإن

$$a^{p-1} \equiv 1 \pmod{p}$$

مبرهنة: إذا كان  $n = p^x$  حيث  $p$  عدداً أولياً و  $x$  عدد صحيح موجب، فإن

فإن

$$\phi(p^x) = p^x - p^{x-1} = p^x \left(1 - \frac{1}{p}\right)$$

$$= p^x (p-1)$$

مجموعة لا فراغ

$$|G| = m$$

$$a \in G$$

حيث  $a$  عدد صحيح

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

② العنصر القانوني

جاء 1

$$\varphi(n) = n \cdot \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right) = n \cdot \prod_{i=1}^k \frac{(p_i - 1)}{p_i}$$

البرهان وجدنا دالة ضربية (نقلها دون برهان)

وبما أن  $p_1, p_2, \dots, p_k$  أعداد مختلفة فكل نسبة أولياً متن متن ومن ثم 1

$$\begin{aligned} \varphi(n) &= \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}) \\ &= \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \dots \varphi(p_k^{\alpha_k}) \end{aligned}$$

$$= p_1^{\alpha_1} \left(1 - \frac{1}{p_1}\right) \cdot p_2^{\alpha_2} \left(1 - \frac{1}{p_2}\right) \dots p_k^{\alpha_k} \left(1 - \frac{1}{p_k}\right)$$

$$= n \left(\frac{p_1 - 1}{p_1}\right) \left(\frac{p_2 - 1}{p_2}\right) \dots \left(\frac{p_k - 1}{p_k}\right)$$

$$= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

$$= \frac{n \prod_{i=1}^k (p_i - 1)}{p_1 \cdot p_2 \dots p_k} = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right)$$

$\varphi(360)$

مثال

360	2
180	2
90	2
45	3
15	3
5	5
1	

$$360 = 2^3 \cdot 3^2 \cdot 5$$

$$\varphi(360) = 360 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right)$$

$$= 360 \left(\frac{1}{2}\right) \left(\frac{2}{3}\right) \left(\frac{4}{5}\right)$$

$$= 96$$

$$Z_{360} = \{0, 1, 2, \dots, 359\}$$

$$|U(Z_{360})| = 96 = \varphi(360)$$

أولنا العدد 360  
مع 360

$$U(Z_{360}) = \{a \in Z_{360} : d(a, 360) = 1\}$$



بعض التمارين البسيطة:

١٠٠

نقسم العدد ١٠٠ إلى ٢٥٦ (نقسم العدد ١٠٠ إلى ٢٥٦)

نتج القسمة ١٠٠ : ٢٥٦ = ٠ ر ١٠٠  
 نتج القسمة ١٠٠ : ٢٥٦ = ٠ ر ١٠٠

العدد ٢٥٦

العدد المطلوب المكون من آحاد وعشرات هو ١٠٠  
 قسمة هذا العدد على ١٠٠

$$3^{256} \equiv k \pmod{100}$$

نلاحظ أن  $d(3, 100) = 1$  حيث  $d(3, 100) = 1$   
 $3^{100} \equiv 1 \pmod{100}$

وبما  $3^{100} \equiv 1 \pmod{100}$   
 $3^{100} = (2^2 \cdot 5^2)^{100}$   
 $= 100 \cdot (1 - \frac{1}{2}) (1 - \frac{1}{5})$   
 $= 100 \cdot (\frac{1}{2}) (\frac{4}{5}) = 40$

إذا كان العدد ١٠٠  
 يمكن كتابته على شكل  
 ١٠٠ = ٢٥٦ + ٢٤

$$256 = 6 \cdot 40 + 16$$

$$3^{256} = (3^{40})^6 \cdot 3^{16} \equiv 1^6 \cdot 3^{16} \pmod{100}$$

$$= (3^4)^4 \pmod{100} \equiv (81)^4 \pmod{100}$$

$$81 + 19 = 100$$

$$\equiv (-19)^4 \pmod{100}$$

$$\equiv [(-19)^2]^2 \pmod{100}$$

$$\equiv (361)^2 \pmod{100}$$

$$\equiv (61)^2 \pmod{100}$$

$$361 = 3 \cdot 100 + 61$$

$$\equiv (61)^2 \pmod{100}$$

$$\equiv (1521) \pmod{100}$$

$$\equiv (15 \cdot 100 + 21) \pmod{100}$$

$$\equiv 21 \pmod{100}$$

أي أن باقي قسمة  $3^{256}$  على ١٠٠ هو ٢١

برهان (5.3) قسم 5.3 مع 100 بعير  
 نأخذ البقرة

$$500 = 5 + 100 + 3$$

إذا كانت الخصائص أكبر من الخصائص نفسها في الخصائص ونأخذ البقرة ونعلم بدالة أول

في تلك الخصائص عددان خصائصهما أوليان فيما بينهما

$$d(n, m) = 1 \text{ و } n, m \in \mathbb{Z}^+$$

$$[m^{g(m)} + n^{g(n)}] \equiv 1 \pmod{n \cdot m}$$

والآن حسب أولي

$$m^{g(m)} \equiv 1 \pmod{n} \Rightarrow n \mid [m^{g(m)} - 1]$$

$$n^{g(n)} \equiv 1 \pmod{m} \Rightarrow m \mid [n^{g(n)} - 1]$$

$n$  و  $m$  أوليان، جداء هذين العددين

$$n \cdot m \mid (m^{g(m)} - 1)(n^{g(n)} - 1)$$

$$n \cdot m \mid \left[ \frac{m^{g(m)} - 1}{n} - \frac{n^{g(n)} - 1}{m} + 1 \right]$$

$$m \mid m^{g(m)}$$

$$\text{و } n \mid n^{g(n)}$$

لدينا

وبالتالي الجداء يقسم الجداء

$$n \cdot m \mid \frac{m^{g(m)}}{n} - \frac{n^{g(n)}}{m}$$

لدينا  $n \cdot m$  يقسم الجداء  $(a)$  و  $n \cdot m$  يقسم الجداء كذلك  
 إذن

$$n \cdot m \mid [1 - m^{g(n)} - n^{g(m)}]$$

$$n \cdot m \mid [n^{g(n)} + m^{g(m)} - 1] \Rightarrow [n^{g(n)} + m^{g(m)}] \equiv 1 \pmod{n \cdot m}$$

وهذا المطلوب



مبرهنة (تقرينة) أويلر  $n > 2$  و  $\varphi(n)$  عدد زوجي دوماً

برهان نفرض أن ناتج تحليل  $n$  لعوامله الأولية (العبارة القانونية)  $n = p_1^{x_1} \cdot p_2^{x_2} \cdots p_k^{x_k}$

$$\varphi(n) = p_1^{x_1-1} \cdot p_2^{x_2-1} \cdots p_k^{x_k-1} \cdot (p_1-1)(p_2-1) \cdots (p_k-1)$$

شروطية دوماً  $(p_1 < p_2 < \cdots < p_k)$

لأن  $p_i$  أولية فردية مختلفة اعتباراً عن  $i=2, \dots$  وبالتالي  $\varphi(n)$  سيكون عدداً زوجياً.

طريقة ثانية لكل تناقض حاسن

(P)  $n = 2^k$  حيث  $k \geq 2$  فإن  $\varphi(2^k) = 2^k - 2^{k-1} = 2^{k-1}(2-1) = 2^{k-1}$  وهو عدد زوجي

(C) إذا لم يكن  $n$  قوة للعدد 2 فهو يقبل القسمة على عدد أولي فردي صحيح  $p$  يقسم  $n$ :

$$n = m \cdot p^s \quad s \geq 1$$

$$d(p, m) = 1 \Rightarrow d(p^s, m) = 1$$

وهي ثم دوماً  $\varphi$  دالة ضربية يكون:

$$\varphi(n) = \varphi(m) \cdot \varphi(p^s) = \varphi(m) \cdot \underbrace{p^{s-1}(p-1)}_{\text{عدد زوجي}}$$

فإن ناتج عدد زوجي.

$$22 \mid \left[ \frac{10 \cdot n + 2}{3} + 5 - 2 \right]$$

طريقة أخرى أويلر العدد

$$22 = 2 \cdot 11$$

إذا كانت الباي هـ يقسم

$$d(3, 22) = 1$$

الكي

$$\varphi(22) \quad 3 \equiv 1 \pmod{22} \Rightarrow 3^{10} \equiv 1 \pmod{22}$$

$$d(5, 22) = 1$$

$$\varphi(22) \quad 5 \equiv 1 \pmod{22} \Rightarrow 5^{10} \equiv 1 \pmod{22}$$

$$[3^{10 \cdot n + 2} + 5^{10 \cdot n + 3}] = [(3^{10})^n 3^2 + (5^{10})^n 5^3 - 2]$$

$$= [(1)^n 3^2 + (1)^n 5^3 - 2] \pmod{22}$$

$$\equiv 0 \pmod{22} \quad \leftarrow (132 \pmod{22})$$

نعمية: أثبت أن العدد  $n$  أولي إذا وفقط إذا كان:

$$n \text{ أولي} \Leftrightarrow n-1 = \varphi(n)$$

الكي: إذا كان  $n$  أولي  $\Rightarrow n-1 = \varphi(n)$

لأن جميع الأعداد الأصغر من  $n$  أولية مع  $n$  اعتباراً من (1)

فهل تحققت  $(n-1) = \varphi(n)$  ؟

نفرض أن  $n-1 = \varphi(n)$

لنثبت أن  $n$  أولي

لو كان  $n$  غير أولي لوجد قسماً  $d$  يقسم  $n$

$$d \mid n : 1 < d < n$$

أي يوجد سبب مجموعة الأعداد  $1, 2, 3, \dots, n-1$

عدد واحد مع السبب ليس أولي مع  $n$  هو  $(d)$  و  $d$  غير أولي

$$\varphi(n) \leq n-2$$

وهذا يتناقض مع الفرض  $\varphi(n) = n-1$

لذلك  $n$  لا يمكن أن يكون غير أولي فلهذا  $n$  عدد أولي



نريد إثبات أن عدد صحيح موجب دالة أولي  $\phi(n)$   $n \in \mathbb{Z}^+$

$$\phi(2n) = \phi(n)$$

$$\phi(2n) = 2\phi(n)$$

إذا كان  $n$  فردياً (1) فإذن

(2)  $n$  زوجي (2) فإذن

$$\begin{aligned} \phi(2n) &= 1 \quad n \text{ فردي} \quad (1) \\ \phi(2n) &= \phi(2) \phi(n) \\ &= 1 \cdot \phi(n) \end{aligned}$$

$$n = 2^k \cdot m \quad ; \quad \phi(2^k, m) = 1 \quad (2) \quad n \text{ زوجي}$$

$$\begin{aligned} \phi(n) &= \phi(2^k) \phi(m) \\ &= 2^{k-1} (2-1) \phi(m) = 2^{k-1} \phi(m) \end{aligned}$$

$$\phi(2n) = \phi(2 \cdot 2^{k+1} \cdot m)$$

$$= \phi(2^{k+1} \cdot m)$$

$$= \phi(2^{k+1}) \phi(m)$$

$$= 2^k (2-1) \phi(m)$$

$$= 2^k \phi(m) = 2 \cdot \underbrace{2^{k-1} \phi(m)}_{\phi(n)}$$

$$= 2 \phi(n)$$

وهو المطلوب